test.au3

especimen

- keylogger
- data mining
- oculta su presencia en el explorador de tareas (usar alternativa - herramientas)

localización física

- HKCU/Microsoft/Windows/CurrentVersion/Run
- carpeta inicio: `shell:startup` → **c:\users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**
- carpeta oculta: **c:\<NOMBRE_EQUIPO>**
- carpeta oculta: **c:\programData\<sha1>**
- carpeta oculta: (capturas log + mining): **c:\users\<user>\appData\Roaming\<sha1>**

herramientas

- Process Explorer, Sysinternals
- cmder, CMD mejorado, portable

extirpación

- eliminar procesos **systeminfo**, **vbc**, mirando previamente su ubicación
- eliminar localizaciones físicas